Amendments to the Claims

1. (Currently amended) A method of providing a time stamping service for setting a client's system clock, comprising the steps of:

a) requesting the time stamping service of a time stamp authority server (TSA) by a service requester based on combination of a time stamping request (TimeStampReq) service message set by a random number and a request message for setting the client's system clock;

b) receiving the time stamping service request from said requester by said time stamp authority server (TSA), ~~and~~ creating a message authentication code (MAC) based on combination of current time (genTime) information and the time stamping request (TimeStampReq) service message in response to the requesting, creating a response message by inserting a message certificate (MacInfo) structure including the message certificate (MAC) into a field of a time stamping response (TimeStampResp) message, and sending ~~a~~ the response message ~~corresponding thereto by said time stamp authority server~~;

c) receiving the response message sent from said time stamp authority server by said requester, creating a message authentication code (MAC) by extracting the current time (genTime) information and the time stamping request (TimeStampReq) service message, which are included in the response message, and verifying the integrity of the response message by comparing the message authentication code (MAC) with another message authentication code (MAC) additionally included in the response message ~~thereof by said requester~~;

d) downloading a certificate revocation list from a directory server by said requester, extracting the current time (genTime) information from the response message transmitted from the time stamp authority server (TSA), and verifying the validity of the certificate revocation list (CRL) by comparing the current time (genTime) information with time information set in the certificate revocation list (CRL) ~~thereof by said requester~~; and

e) downloading a certificate for an electronic signature of said time stamp authority server from said directory server by said requester, verifying validity of the time

stamp response (TimeStampResp) service message, ~~an electronic signature value thereof~~ and, if the time stamp response (TimeStampResp) service message is valid, setting the client's system clock using the current time (genTime) information extracted from the response message ~~in accordance with the verified result by said requestor~~.

2. (Original) The method as set forth in claim 1, wherein said step a) includes the steps of:

a-1) generating a random number with a given value and setting it as a nonce value of a service request message (TimeStampReq);

a-2) setting a requestType parameter of said TimeStampReq message to a getBaseTime value and adding the resulting structure to an extension field of said TimeStampReq message to inform said time stamp authority server that the service request is for the setting of said client's system clock; and

a-3) filling other parameters of said TimeStampReq message with given values and sending the resulting TimeStampReq message to said time stamp authority server.

3. (Original) The method as set forth in claim 1, wherein said step b) includes the steps of:

b-1) receiving a service request message (TimeStampReq) sent from said requester and authenticating and verifying the received TimeStampReq message;

b-2) if there is an error at said step b-1), processing the received TimeStampReq message as an erroneous message, sending the processed result to said requester and ending the corresponding process;

b-3) if there is no error at said step b-1), filling parameters of the response message (TimeStampResp) with given values;

b-4) extracting a TSTInfo structure from a TimeStampResp message structure created at said b-3) and, in turn, current time information (a genTime value) from the extracted TSTInfo structure, calculating a message authentication code (MAC) value on the basis of the extracted genTime value and a nonce value, set by said requester and contained in said TimeStampReq message, and setting the calculated MAC value and identifier information of an algorithm used for the calculation of the MAC value

respectively in corresponding fields of a MacInfo structure to assure the integrity of said response message;

b-5) adding the resulting MacInfo structure to an extension field of said TSTInfo structure and thus completing the creation of said TimeStampResp message structure; and b-6) sending the completed response message (TimeStampResp) to said requester.

4. (Original) The method as set forth in claim 1, wherein said step c) includes the steps of:

c-1) receiving the response message (TimeStampResp) sent from said time stamp authority server and authenticating and verifying the received response message;

c-2) extracting a TSTInfo structure from said TimeStampResp message and, in turn, current time information (a genTime value) from the extracted TSTInfo structure, finding a nonce value, set by said requester and sent to said time stamp authority server, and directly calculating a message authentication code (MAC) value on the basis of the extracted genTime value and the found nonce value to check the integrity of said TimeStampResp message;

c-3) extracting a MacInfo structure from said TimeStampResp message sent from said time stamp authority server and, in turn, a MAC value from the extracted MacInfo structure and comparing the extracted MAC value with said MAC value calculated at said step c-2) to determine whether the two MAC values are equal; and c-4) if said two MAC values are not equal, recognizing that the current time information (genTime value) sent from said time stamp authority server was altered during the sending and said client's system clock cannot thus be set and then processing the received response message as an erroneous message, and if said two MAC values are equal, recognizing that the integrity of the received response message has been assured.

5. (Original) The method as set forth in claim 1, wherein said step d) includes the steps of:

d-1) downloading said certificate revocation list and said certificate for the electronic signature of said time stamp authority server from said directory server managing certificates of all objects and said certificate revocation list;

d-2) extracting time information set to thisUpdate and nextupdate values from said certificate revocation list downloaded from said directory server, so as to verify the validity of said certificate revocation list on the basis of a genTime value contained in the response message sent from said time stamp authority server; and

d-3) determining whether said genTime value is present between said thisUpdate and nextupdate values, so as to determine whether said certificate revocation list is valid, and if said certificate revocation list is not valid, recognizing that a signature value sent from said time stamp authority server cannot be verified and said client's system clock cannot thus be set and then performing an associated error process.

6. (Original) The method as set forth in claim 1, wherein said step e) includes the steps of:

e-1) extracting desired information from said certificate for the electronic signature of said time stamp authority server and checking whether a serial number of said certificate of said time stamp authority server among the extracted information is present in said certificate revocation list, so as to verify the validity of said certificate;

e-2) if the serial number of said certificate of said time stamp authority server is present in said certificate revocation list, recognizing that said client's system clock cannot be set and then performing an associated error process;

e-3) extracting a public key from said certificate of said time stamp authority server if the serial number of said certificate is not present in said certificate revocation list;

e-4) extracting a signature value from a SignerInfo structure of said TimeStampResp message, decoding the extracted signature value using the extracted public key, extracting a first hash value from the decoded result and directly calculating a second hash value using a digest algorithm of said SignerInfo structure;

e-5) comparing said first and second hash values with each other to determine whether they are equal, if said first and second hash values are not equal, recognizing

that said time stamp authority server sending said TimeStampResp message is not valid and then performing an associated error process, and if said first and second hash values are equal, recognizing that said time stamp authority server sending said TimeStampResp message is valid; and

e-6) setting said client's system clock on the basis of a genTime value extracted from said TimeStampResp message.